PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 23 September 1999 (23.09.99)	
International application No.: PCT/DE99/00415	Applicant's or agent's file reference: GR 98 P 1347P
International filing date: 16 February 1999 (16.02.99)	Priority date: 16 March 1998 (16.03.98)
Applicant: ENTERROTTACHER, Anton et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

09 August 1999 (09.08.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GR 98 P 1347P	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DE99/00415	International filing date (*day/month/year*) 16 February 1999 (16.02.99)	Priority date (*day/month/year*) 16 March 1998 (16.03.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

RECEIVED
NOV 22 2000
Technology Center 2100

Date of submission of the demand 09 August 1999 (09.08.99)	Date of completion of this report 24 January 2000 (24.01.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE99/00415

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-5, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-3, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE 99/00415

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-3	YES
	Claims		NO
Inventive step (IS)	Claims	1-3	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-3	YES
	Claims		NO

2. Citations and explanations

The international application concerns a method for the authentication of key devices.

The closest prior art is document WO-A-95 14283. In that document, the public key and the address of a user are certified and key creation is undertaken using secure connections on the basis of keying material and the administrator's password.

The remaining documents in the international search report merely contain more general prior art with respect to the certification of key devices.

So as to secure the authenticity of the communication partner in a connection with a key device, as per Claim 1 of the international application, each individually certified key device is allocated a group-specific signature code and a group-specific signature of the certificate.

This substantive matter is not disclosed by the documents of the international search report either individually or in combination, nor is it obvious therefrom. Therefore, novelty and inventive step are acknowledged.

This also applies to dependent Claims 2 and 3.

Industrial applicability is also established for the operation of key devices with asymmetrical coding methods.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The description does not cite document D1, nor does it indicate the relevant prior art disclosed therein (PCT Rule 5.1(a)(ii)).

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES INTERNATIONALEN RECHERCHENBERICHTS ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

An
SIEMENS AG
z.H. JAHNEN, Georg.
Postfach 22 16 34
D-80506 München
GERMANY

GR ZD VM Mch M
Eing. 02. AUG. 1999
GR
Frist

Aktenzeichen des Anmelders oder Anwalts GR 98 P 1347P	Absendedatum *(Tag/Monat/Jahr)* 29/07/1999
Internationales Aktenzeichen PCT/DE 99/ 00415	**WEITERES VORGEHEN** siehe Punkte 1 und 4 unten
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 16/02/1999

1. [X] Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

   Einreichung von Änderungen und einer Erklärung nach Artikel 19:
   Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

   Bis wann sind Änderungen einzureichen?

   Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

   Wo sind Änderungen einzureichen?

   Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20, Telefaxnr.: (41-22) 740.14.35

   Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. [ ] Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.

3. [ ] **Hinsichtlich des Widerspruchs** gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

   [ ] der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

   [ ] noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

   Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90 bis.1 bzw. 90 bis.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

   Innerhalb von **19 Monaten** seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

   Innerhalb von **20 Monaten** seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Annick Crab

(Siehe Anmerkungen auf Beiblatt)

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.
Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Anspruche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen, die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunumerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der dieinternationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

PNSPOCID: -XSISA220NODER1-

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

i) der Anspruch unverändert ist;

ii) der Anspruch gestrichen worden ist;

iii) der Anspruch neu ist;

iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;

v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]: "Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."

2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]: "Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."

3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]: "Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt."Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."

4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]: "Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amts sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

BNSDOCID: <XSISA220NODER4>

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
GR 98 P 1347P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/DE 99/ 00415	16/02/1999	16/03/1998
Anmelder		
SIEMENS AKTIENGESELLSCHAFT et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

[ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

[ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

[ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

[ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

[ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

[ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

[ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

[X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

[ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

[X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

[ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

[ ] wie vom Anmelder vorgeschlagen [X] keine der Abb.

[ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

[ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 99/00415

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 97 48208 A (ERICSSON TELEFON AB L M) 18. Dezember 1997 (1997-12-18) Zusammenfassung Seite 5, Zeile 22 - Zeile 29 Seite 6, Zeile 7 - Seite 7, Zeile 6 Abbildungen 1,2,4 ---	1,2
A	FR 2 709 903 A (THOMSON CSF) 17. März 1995 (1995-03-17) Zusammenfassung Seite 4, Zeile 10 - Zeile 34 Seite 6, Zeile 1 - Zeile 8 Anspruch 1 Abbildungen 1-3 --- -/--	1,3

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
21. Juli 1999	29/07/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 99/00415

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 95 14283 A (HUGHES AIRCRAFT CO) 26. Mai 1995 (1995-05-26) Seite 1-4 Abbildung 1 -----	1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 99/00415

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9748208 A	18-12-1997	US 5729537 A	17-03-1998
		AU 3199697 A	07-01-1998
		CA 2258036 A	18-12-1997
		EP 0904643 A	31-03-1999
FR 2709903 A	17-03-1995	KEINE	
WO 9514283 A	26-05-1995	AU 669828 B	20-06-1996
		AU 8095794 A	06-06-1995
		CA 2149744 A,C	09-05-1995
		EP 0682832 A	22-11-1995
		JP 2723365 B	09-03-1998
		JP 8512445 T	24-12-1996
		NO 952584 A	27-06-1995
		US 5825300 A	20-10-1998

Beschreibung

Authentifizierung von Schlüsselgeräten

Die Erfindung betrifft ein Verfahren gemäß dem Oberbegriff des Patentanspruchs 1.

Ein solches Verfahren ist im Prinzip in dem Buch von W. Fumy und H.P. Rieß: Kryptographie, Entwurf und Analyse symmetrischer Kryptosysteme R. Oldenbourg Verlag, München Wien, 1988, ISBN 3-486-20868-3, beschrieben.

Bei verschlüsselter Übertragung von Sprache oder allgemeiner von Daten müssen beide Kommunikationspartner über ein gemeinsames Geheimnis verfügen, das Schlüsselwort. Dieses Schlüsselwort ist einem potentiellen Mithörer oder Gegner unbekannt. Eine Möglichkeit hierfür ist ein asymmetrisches Verschlüsselungsverfahren, bei dem Zufallszahlen zwischen den Kommunikationspartnern ausgetauscht und daraus gemeinsame Schlüsselworte gebildet werden.

Bei diesem Verfahren kann nicht festgestellt werden, ob die verschlüsselte Verbindung zu dem gewünschten Kommunikationspartner oder zu einem Gegner aufgebaut wird.

Kryptographische Verfahren können nicht nur zu Geheimhaltung, sondern auch zur Authentifizierung von Nachrichten eingesetzt werden. Die Verschlüsselung einer Nachricht unter Verwendung eines Schlüsselwortes beinhaltet im Prinzip auch deren Authentizität, da ein Gegner ohne Kenntnis des Schlüsselwortes den Klartext der Nachricht nicht erzeugen kann.

Bei einem asymmetrischen Kryptosystem wird für die Verschlüsselung einer Nachricht ein anderes Schlüsselwort verwendet, als für die Entschlüsselung. Ein solches System mit einem öffentlichen und einem privaten Schlüssel wird auch als Public Key System bezeichnet. Das bekannteste Beispiel für das Pu-

blic Key System ist das sogenannte RSA-Verfahren, dessen Grundzüge ebenfalls in der eingangs genannten Literaturstelle beschrieben sind.

Auf den ersten Blick wird das System der Schlüsselverteilung bei der Verwendung asymmetrischer Kryptosysteme weitgehend gelöst, da die öffentlichen Schlüssel problemlos über unsichere Datenkanäle ausgetauscht werden können. Dies ist aber nur richtig, solang man das Abhören als die einzige Gefährdung einer Kommunikationsverbindung betrachtet. Neben passiven Abhörversuchen muss man in den meisten Fällen aber auch mit der Möglichkeit aktiver Angriffe rechnen. Hierbei schaltet sich ein aktiver Gegner in die Datenverbindung zwischen zwei Teilnehmer ein. Ein solcher Angriff kann nur bei Verwendung von Authentifizierungsmaßnahmen erkannt werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren anzugeben, durch das die an einem Datenaustausch beteiligten Schlüsselgeräte authentifiziert werden können.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Im Folgenden wird die Erfindung anhand eines Ausführungsbeispieles beschrieben. Bei der Beschreibung werden folgende Abkürzungen verwendet:

E	Verschlüsselung
D	Entschlüsselung
A, B, X	Teilnehmer
AD	Administrator
p	öffentlicher Schlüssel
s	geheimer Schlüssel
pAD	Signaturschlüssel, entspricht dem öffentlichen Schlüssel p des Administrators AD

Z	Zertifikat, entspricht dem öffentlichen Schlüssel p, dem Namen und weiteren Angaben eines Teilnehmers X
S	Signatur
S(Z)	Signatur des Zertifikates Z

Die Erfindung geht von einem Kryptoverfahren aus, bei dem alle Verschlüsselungsgeräte mit einem gemeinsamen Public Key Schlüssel ausgestattet sind. Dieser öffentliche Schlüssel pAD wird von einer vertrauenswürdigen Instanz, einem sogenannten Administrator AD vergeben. Hierdurch kann prinzipiell jedes Gerät mit jedem kommunizieren, wobei die teilnehmenden Geräte authentifiziert sind.

In an sich bekannter Weise ist jedem Schlüsselgerät individuell ein Zertifikat Z zugeordnet, praktisch eine Art Name für dieses Gerät. Daneben enthält das Zertifikat Z, bei der Verwendung des Public-Key-Systems, den öffentlichen Schlüssel pX des Teilnehmers oder Benutzers X.

Erfindungsgemäß werden Benutzergruppen gebildet, deren Geräte mit einem gemeinsamen, gruppenspezifischen Signaturschlüssel pAD ausgestattet werden. Dieser Signaturschlüssel pAD ist der öffentliche Schlüssel pAD des Administrators AD. Er kann direkt im Gerät, oder er kann in Form anderer Speichermedien, beispielsweise auf Chipkarte, gespeichert sein. Eine solche Benutzergruppe weist eine beschränkte Anzahl von Teilnehmern auf. Hierdurch ist die Verbreitung des Signaturschlüssels pAD eingeschränkt.

In an sich bekannter Weise kann beim Administrator AD zu einem Zertifikat Z(X) eines Benutzers X eine Signatur S(Z(X)) erzeugt werden. Dabei wird das Zertifikat Z(X) mit dem geheimen Schlüssels sAD des Administrators AD verschlüsselt.

$$S(Z(X))=E(Z(X),sAD)$$

Diese Signatur S(Z(X)) wird ebenfalls im Schlüsselgerät des Benutzers X fest oder mobil gespeichert.

Der geheime und der öffentliche Schlüssel sAD, sX und pAD, pX des Administrators AD beziehungsweise der Teilnehmer X sind Teil des Public Key Systems, das beispielsweise durch die RSA-Algorithmen realisiert ist.

Der gruppenspezifische Signaturschlüssels pAD und die teilnehmerspezifische beziehungsweise gerätespezifische Signatur S(Z(X)) werden beispielsweise bei einer Ausgestaltung der Erfindung bei einer Erstinitalisierung auf das Schlüsselgerät geladen. Daneben ist im Schlüsselgerät das zugehörige Zertifikat Z(X) gespeichert. Diese Daten können auch an den entsprechenden Teilnehmer auf einer Chipkarte ausgehändigt werden. Für diese Vorgänge ist ein persönlicher Kontakt mit dem Administrator AD oder zumindest ein sicherer Übertragungskanal zu ihm notwendig.

Zur gesicherten Kommunikation wird eine Verbindung zwischen den Teilnehmern A und B, das heißt zwischen den zugehörigen Schlüsselgeräten aufgebaut. Der Teilnehmer A überträgt zum Teilnehmer B das Zertifikat Z(A) und die Signatur S(Z(A)). Der Teilnehmer B kann unter Verwendung des Signaturschlüssels pAD, das heißt des öffentlichen Schlüssels p des Administrators AD, die Echtheit des Zertifikates Z(A), das heißt die Echtheit des Teilnehmers A verifizieren:

$$D(S(Z(A)),pAD)=D(E(Z(A),sAD),pAD)=Z(A)$$

Analog überprüft der Teilnehmer A den Teilnehmer B.

Ein potentieller Angreifer ist gruppenfremd, besitzt keine vom Administrator AD ausgestellte Signatur S, und kann daher zu keinem Teilnehmer dieser Gruppe eine Verbindung aufbauen,.

Bei einem Diebstahl werden die entsprechenden Geräte von der Benutzergruppe ausgeschlossen, so daß sie für einen Angreifer unbrauchbar werden. Hierzu ist bei einer möglichen Ausgestaltung der Erfindung im Schlüsselgerät eine Liste der zugelassenen Teilnehmer beziehungsweise der Schlüsselgeräte gespeichert. Es können die Identitäten der möglichen Schlüsselgeräte hinterlegt sein, und in den Verbindungsaufbau ist eine entsprechende Sicherheitsabfrage integriert.

Patentansprüche

1. Verfahren zur Authentifizierung von Schlüsselgeräten unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens, bei dem dem Schlüsselgerät ein geräteindividuelles Zertifikat (Z) zugeordnet wird,
dadurch gekennzeichnet,
dass jedem Schlüsselgerät ein gruppenspezifischer Signaturschlüssel (pAD) und eine gruppenspezifische Signatur (S(Z)) des Zertifikats (Z) zugeordnet wird, wobei eine Gruppe aus einer zahlenmäßig begrenzten Anzahl von Schlüsselgeräten besteht.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Signaturschlüssel (pAD) und die Signatur (S(Z)) bei einer einmaligen Erstinitialisierung vergeben wird.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass die Gruppenzugehörigkeit durch Vergleich mit einer Liste ermittelt wird.

Zusammenfassung

Authentifizierung von Schlüsselgeräten

Die Erfindung betrifft ein Verfahren zur Authentifizierung von Schlüsselgeräten unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens, bei dem dem Schlüsselgerät ein geräteindividuelles Zertifikat (Z) zugeordnet wird. Erfindungsgemäß ist jedem Schlüsselgerät ein gruppenspezifischer Signaturschlüssel (pAD) und eine gruppenspezifische Signatur (S(Z)) des Zertifikats (Z) zugeordnet, wobei eine Gruppe aus einer zahlenmäßig begrenzten Anzahl von Schlüsselgeräten besteht.